UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/751,300	01/02/2004	Pasi Eronen	944-4.40	8800

4955 7590 05/01/2007

WARE FRESSOLA VAN DER SLUYS &
ADOLPHSON, LLP
BRADFORD GREEN, BUILDING 5
755 MAIN STREET, P O BOX 224
MONROE, CT 06468

EXAMINER	
LE, CANH	

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
05/01/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/751,300	ERONEN ET AL.	
	Examiner	Art Unit	
	Canh Le	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 January 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01/02/2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *04/19/2004; 04/05/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This Office Action is in response to the application filed on 01/02/2004. Claims 1-7 are pending and have been examined.

Specification

The disclosure is objected to because of the following informalities: the acronyms

In the specification, there are some acronyms: UMTS (page 6, line 4), MWLAN, and MGSM (page 6, line 33) do not spell out for the first use. Appropriate correction is required.

Drawings

The drawings are objected to in figure 1 because the Examiner believes that the arrow pointer from "Other terminal components" to box 14. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional

replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 5 is a computer program product and it depends on method the claim 1. It is not clear that this is a computer program product or method claim. This ambiguity renders claim 5 indefinite.

Claim 7 is system claim and it depends on claim 6. It is not clear that it is a apparatus claim or system claim. This ambiguity renders claim 7 indefinite.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 1-3 and 5-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sarvar Patel, "Analysis of EAP-SIM Session Key Agreement", IETF EAP mailing, May 29, 2003, pp. in view of Dharmapurika et al., "Longest Prefix Matching Using Bloom Filter", SIGCOMM'03, August 25-29, 2003, pp. 201-212.

As per claim 1:

Patel teaches a method by which a terminal (10) determines whether a candidate RAND included in a RAND challenge is a member of a set of previously used RANDs **[pg. 1 to pg. 4].**

Patel does not teaches "a step (31) of encoding the previously ..."

Dharmapurika teaches:

a step (31) of encoding the previously used RANDs using a data structure (21) consisting of an ordered set of components having component values derived from the previously used RANDs wherein each component has a value of one or zero depending on whether it is pointed to by one or more pointers each having a value based on a digest of all the bits of a

respective previously used RAND or having a value otherwise derived from all the components of a respective previously used RAND so that in either case all bits of the RAND contribute in determining the value of the component **[pg. 203, Bloom Filter Theory section to pf. 204, section Counting Bloom filter]**; and

a step (32) of checking the data structure (21) to determine whether the data structure indicates whether the candidate RAND is a member of a set of previously used RANDs **[pg. 203, Bloom Filter Theory section to pg. 204, section Counting Bloom filter]**;

wherein the data structure (21) is such as to at least provide a true answer as to whether the candidate RAND is not an element of the set of previously used RANDs **[pg. 203, section 3. BLOOM FILTER THEORY to pg. 204, section 3.2 Counting Bloom Filters; "If at least one of the k bits is 0, then the message is declared to be a non-member of the set"]**.

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the method of Patel of the invention by including the step of Dharmapurikar because It would provide efficient using Bloom filter which is an efficient data structure for membership queries with tunable false positive errors **[Dharmapurikar, pg. 201, col. 2, par. [2], lines 1-5]**.

As per claim 2:

Dharmapurikar further teaches a method as in claim 1, wherein in the step (31) of encoding the previously used RANDs, a set of hash functions is used

each having a range equal to the number of components of the data structure (21), and for each previously used RAND, each of the hash functions is evaluated and the component in the ordered set of components at the position indicated by the hash function value is set to one **[pg. 203, section 3. BLOOM FILTER THEORY to pg. 204, section 3.2 Counting Bloom Filters; "For each message x_i in X ... m-bit causes k bits in the m-bit vector to be set to 1"]**.

As per claim 3:

Dharmapurikar further teaches a method as in claim 2, wherein the previously used RAND values serve as the hash functions based on using the RAND values as pointers to components of the data structure (21) **[pg. 203, section 3. BLOOM FILTER THEORY to pg. 204, section 3.2 Counting Bloom Filters; "For each message x_i in X ... m-bit causes k bits in the m-bit vector to be set to 1"; pg. 211, fig. 10a; H1 is a pointer which point to m bits vectors of Boom filter]**.

As per claim 5:

it is essentially the same as claim 1 except that it sets forth the claimed invention as a computer program product rather a method and rejected under the same reasons as applied above.

As per claim 6:

it is essentially the same as claim 1 except that it sets forth the claimed invention as an apparatus rather a method and rejected under the same reasons as applied above.

As per claim 7:

it is essentially the same as claim 1 except that it sets forth the claimed invention as a system rather a method and rejected under the same reasons as applied above.

Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sarvar Patel, "Analysis of EAP-SIM Session Key Agreement", IETF EAP mailing, May 29, 2003, pp. in view of Dharmapurika et al., "Longest Prefix Matching Using Bloom 7Filter", SIGCOMM'03, August 25-29, 2003, pp. 201-212 and further in view of Aguilera et al. (US 2005/002209 A1).

As per claim 4:

Dharmapurikar further teaches a method as in claim 1, wherein the data structure (21) is a multi-part data structure (21) with each part having an upper limit on the number of RAND values it can indicate as belonging to the set of previously used RAND values **[pg. 211, fig. 10b; there are Bloom Filters of length m/2].**

Patel and Dharmapurikar do not explicitly teach wherein when an upper limit is reached for one of the parts, another of the parts is reset.

Aguilera teaches wherein when an upper limit is reached for one of the parts, another of the parts is reset **[par. [0014], lines 8-14].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the method of Patel and Dharmapurika of the invention by including the step of Aguilera because It would provide a simple solution that would be to reset the Bloom filter to an empty state **[Aguilera, par. [0014], lines 12-13].**

Conclusion

The prior arts made of record and not relied upon are considered pertinent to applicant's disclosure.

U.S. Patent No. 6,920,477 B2 to Mitzenmacher, Michael;

U.S. Patent Application Publication No. 2004/0162105 A1 to Reddy et al.;

U.S. Patent Application Publication No. 2005/0108368 A1 to Mohan et al.;

H. Haverinen and J. Salowey (editor). EAP SIM Authentication, February 2003, http://www.ietf.internet-drafts/draft-haverinen-pppext-eap-sim-10.txt

B. H. Bloom. Space/Time Trade-offs in Hash Coding with Allowable Errors, Communications of ACM, Vol. 13, No 7, July 1970, 422-426.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Canh Le whose telephone number is 571-

270-1380. The examiner can normally be reached on Monday to Friday 7:30AM to 5:00PM other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TAGHI ARANI
PRIMARY EXAMINER
4/27/07

Canh Le

April 23, 2007